



Beosin

Follow

Apr 9 · 5 min read · Listen

Save



Blockchain Security Monthly Recap of March: \$218M lost in attacks



It's time for our monthly security report! According to Beosin EagleEye security risk monitoring, warning, and blocking platform, in March 2023, the number of various security incidents and the amount involved increased significantly compared with February. In this month, more than 21 typical security incidents occurred and the total loss of various security incidents was about 218 million US dollars, which is up about 283% compared with last month and 6.6 million US dollars are lost because of rug pulls.

The biggest security incident in January was the attack on LendHub, a HECO cross-chain lending platform, which caused a loss of 6 million dollars because LendHub did not make its old-version contract deprecated. In addition, there were two cases of personal wallet theft and the loss of each case was more than a million dollars. Wallet security still deserves everyone's attention.

The main amount of losses came from a loss of \$197 million in the attack on Euler Finance on March 13. Up to now, the attacker has refunded \$150 million of the stolen funds. The second largest security incident was that SafeMoon introduced a vulnerability of burning tokens arbitrarily after its smart contract upgrade, and the loss was up to \$8.9 million. Two typical phishing incidents targeting users occurred this month, and the losses were more than \$1 million. In addition, a rug pull occurred on Kokomo Finance, a lending protocol built on Optimism, and the deployer took away \$4 million, which has been the largest rug pull recently.

DeFi

『 8 』 Typical Security Incidents

№1 On March 6, When PeopleDAO collected monthly contributors by Google Form, hackers stole 76 \$ETH (about \$120,000) through social engineering attacks.

№2 On March 7, Tender.Fi, a lending protocol, was attacked due to an error in its oracle contract and suffered a loss of \$1.58 million.

№3 On March 9, Hedera suffered an attack on its smart contract, losing about \$600,000.

№4 On March 13, Euler Finance, a lending protocol, suffered a flash loan attack with a loss of \$197 million. Up to March 28, the attacker has refunded \$150 million.

№5 On March 15, Poolz Finance was attacked on ETH, BSC, and Polygon, losing about \$500,000.

№6 On March 22, Nuwa was attacked by a front-run attack of an MEV bot with a loss of about \$110,000.

№7 On March 29, SafeMoon introduced a vulnerability of burning tokens arbitrarily after its smart contract upgrade. It was attacked by a front run attack of an MEV bot and the loss was up to \$8.9 million.

№8 On March 29, UNMS, a BSC-based project, was attacked with a loss of about \$100,000.

NFT

『 2 』 Typical Security Incidents

№1 On March 1, Monkey Drainer, announced that it would shut down its service. In its final message, it said that young cyber criminals should not lose themselves in the pursuit of easy money. Since the end of 2022, the team has stolen at least \$16 million worth of NFT assets.

№2 On March 16, ParaSpace, an NFT lending platform, was attacked and luckily the attack was blocked and 2,909 \$ETH were saved. The final loss was 50–150 \$ETH.

Wallet Security

『 2 』 Typical Security Incidents

№1 On March 24, an Ethereum address was under a phishing attack by ERC20 Permit and lost \$4,000,000.

№2 On March 30, Patricio Worthalter, founder of POAP, was under a phishing attack and lost about \$3,700,000.

Rug Pull/Crypto Scam

『 6 』 Typical Security Incidents

№1 On March 2, ArbiSwap, an Arbitrum-based dex, had a rug pull and the contract deployer made a profit of \$138,000.

№2 On March 8, ProTradex, a BSC project, had a rug pull and the contract deployer made a profit of about \$600,000 and transferred the fund to Tornado Cash.

№3 On March 13, \$BCGA token had a rug pull and the contract deployer made a profit of \$39,092.

№4 Harvest Keeper, a DeFi protocol, maliciously transferred users' funds. The attacker used owner privilege to make a profit of \$930,000.

№5 On March 21, Thunder Lands had a rug pull and the deployer made a profit of \$70,000.

№6 On March 27, Kokomo Finance, a lending protocol built on Optimism, had a rug pull and the total loss was \$4,000,000.

Crypto Crime

『2』 Typical Security Incidents

№1 In March, India's Enforcement Directorate was investigating "several" crypto cases for money-laundering schemes and has seized \$115.5 million in such crimes.

№2 On March 23, the Xinyi Procuratorate filed a public prosecution against Ubank scam with a pyramid scheme transaction volume of more than 10 billion yuan.

Others

『1』 Typical Security Incidents

№1 On March 17, General Bytes, a Bitcoin ATM maker, was under a zero-day hack. A hacker gained access to users' funds from hot wallets and stole \$1,800,000 worth of crypto assets.



In view of the current new situation in the field of blockchain security, Beosin concludes:

Generally, in March 2023, the number of various security incidents and the amount involved increased significantly compared with February. The total loss of various security incidents was about 218 million US dollars, which is up about 283% compared with last month.

The number of rug pulls and the amount of loss have increased significantly compared with last month. Users are advised to be more careful and conduct a detailed background investigation of projects. Phishing attacks are still the main reason for security incidents this month. Users are advised to check carefully before signing or authorizing and verify the entire address of the receiver before transferring money. 60% of the attacks this month were due to the exploitation of smart contract vulnerabilities. It is recommended that the project teams must seek a professional security company for audit before launching their projects. Users should also carefully check the audit report before interacting with a project to avoid potential loss.

Beosin is a leading global blockchain security company co-founded by several professors from world-renowned universities and there are 40+ PhDs in the team. It has offices in Singapore, Korea, Japan, and other 10+ countries. With the mission of “Securing Blockchain Ecosystem”, Beosin provides “All-in-one” blockchain security solution covering Smart Contract Audit, Risk Monitoring & Alert, KYT/AML, and Crypto Tracing. Beosin has already audited more than 3000 smart contracts and protected more than \$500 billion funds of our clients.